CLAIMS

What is claimed is:

1. An electronic transaction verification system for use at a location where a transaction token is presented by an individual comprising:

a transaction information database for storing an account information for an authorized user;

a reading device for reading and transmitting transaction information data to the information database;

a biometric data device for scanning and transmitting biometric data with the transaction information to the information database;

wherein the biometric data device selectively transmits biometric data to the biometric database for comparison with the biometric data stored for the authorized user to verify the identity of the individual presenting the transaction token; and

wherein the reading device selectively transmits transaction information data to the information database for comparison with account information stored for the authorized user to verify a condition of the account.

2. The system of claim 1 further comprising:

a signature scanning device for scanning signature data received with the transaction information;

a signature database for storing signature data for the authorized user; and

wherein the signature scanning device selectively transmits signature data to the signature database for comparison with the signature stored for the authorized user.

3. The system of claim 1 wherein the transaction token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, travelers check, and a food stamp.

4. The system of claim 1 wherein the biometric data is any one of a fingerprint scan, retinal scan, an iris scan, a voice print, a hand geometry scan, or a facial scan.

5. The system of claim 3 wherein the transaction information data includes data written in magnetic ink on the check.

6. The system of claim 3 wherein the transaction information data includes data encoded on the transaction token.

7. The system of claim 1 wherein the electronic transaction verification system selectively returns a report on customer usages.

8. The system of claim 1 wherein the biometric data device further selectively encodes recorded biometric data on the transaction token.

9. The system of claim 8 wherein the recorded biometric data is any one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry or a facial scan.

10. The system of claim 1 wherein the reading device and the biometric data device are located remotely from the biometric database and the transaction information database.

11. The system of claim 1 wherein the reading device and the biometric data device are located in proximity to the biometric database and the transaction information database.

12. The system of claim 1 further comprising an additional biometric database for storing biometric data for a plurality of invalid users.

13. The system of claim 12 wherein the biometric data is transmitted to the additional biometric database to determine if the individual presenting the transaction token is an invalid user.

14. An electronic transaction verification system for use at a location were a transaction token is presented by an individual, comprising:

a transaction information database for storing an account information for an authorized user;

reading means for reading and transmitting transaction information data to the information database;

biometric data means for recording and transmitting biometric data received with the transaction information data to the information database;

a biometric database for storing biometric data for the authorized user;

wherein the reading means selectively transmits transaction information data to the transaction information database for comparison with account information for the authorized user to verify a condition of the account; and

wherein the biometric data means selectively transmits biometric data to the biometric database for comparison with the biometric data stored for the user to verify the identity of the individual presenting the transaction token.

15. The system of claim 14 further including:

signature scanning means for scanning signature data received with the transaction information;

a signature database for storing signature data for the authorized user; and

wherein the signature scanning means selectively transmits signature data to the signature database for comparison with the signature stored for the authorized user.

16. The system of claim 14 wherein the transaction token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, a travelers check and a food stamp.

17. The system of claim 16 wherein the transaction information data includes data written in magnetic ink on the check.

18. The system of claim 16 wherein the transaction information data includes data encoded on the transaction token.

19. The system of claim 14 further including report means for transmitting a report detailing customer usage of the electronic transaction verification system.

20. The system of claim 14 further including means for selectively encoding the biometric data from the biometric data means in a readable medium on the transaction token.

21. The system of claim 14 wherein the biometric data is any one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry scan, or a facial scan.

22. The system of claim 14 further comprising an additional biometric database for storing biometric data for a plurality of invalid users.

23. The system of claim 22 wherein the biometric data is transmitted to the additional biometric database to determine if the individual presenting the transaction token is an invalid user.

24. A method of verifying the identity of a person attempting to tender a transaction token, and the condition of an account against which the transaction token is applied, the method comprising the steps of:

obtaining transaction information from the transaction token;

obtaining biometric data from the person tendering the transaction token;

selectively transmitting the transaction information to a transaction information database that stores an account information for an authorized user;

comparing the transmitted transaction information with the account information stored in the transaction information database to determine if the account against which the transaction token is applied is in condition to satisfy the transaction;

selectively transmitting the biometric data to a biometric database that stores biometric information for the authorized user;

comparing the transmitted biometric data with biometric information stored in the biometric database to determine if the person tendering the transaction token is authorized to use the account against which the transaction token is applied.

25. The method of claim 24, further including the steps of:

obtaining the signature of the person tendering the transaction token;

selectively transmitting the signature information, either together with or separately from the transaction information and the biometric data, to a signature database that stores signature information for the authorized user;

comparing the transmitted signature information with signature information in the signature database to determine if the signature is that of an authorized user for the account against which the transaction token is applied.

26. The method of claim 24 further including the step of encoding the biometric data on the transaction token.

27. The method of claim 24 further including the step of transmitting data indicative of whether the person is authorized to use the account to the location where the transaction information and biometric data are obtained.

28. An electronic transaction verification system for use with a transaction token processing system, at a location where a transaction token is presented by an authorized user, comprising:

a reading device for reading and transmitting transaction information to the transaction information database;

a biometric data device for recording and transmitting biometric data that is received with the transaction token;

a biometric database for storing biometric data for a plurality of authorized users;

a transaction information database for storing account information for an authorized user;

wherein the biometric device selectively transmits biometric data to the first biometric database to verify the identity of the individual presenting the transaction token; and

wherein the reading device selectively transmits the transaction information to the transaction information database to verify the condition of the account.

29. The electronic transaction verification system for use with a transaction token processing system of claim 28 further comprising an additional biometric database for storing biometric data for a plurality of invalid users.

30. The electronic transaction verification system for use with a transaction token processing system of claim 28 wherein the transaction information comprises magnetic ink character recognition data that is printed on the negotiable instrument.

31. The electronic transaction verification system for use with a transaction token processing system of claim 28 wherein the biometric data device digitizes a representation of the biometric data received with the transaction information and encodes the digitized biometric data directly on the transaction token.

32. The electronic transaction verification system for use with a transaction token processing system of claim 29 wherein the biometric data is transmitted to the additional biometric database to determine if the individual presenting the transaction token is an invalid user.

33. The electronic transaction verification system for use with a transaction token processing system of claim 28 further comprising:

a scanning device for scanning signature data received with the negotiable instrument;

a signature database for storing signature data for the authorized user;

wherein the scanning device selectively transmits signature data to the signature database to determine if the signature data was received from the authorized user.